Louisiana Law Review

Volume 64 | Number 4
Normalization of National Security Law: A Symposium
Summer 2004

FOIA and Fighting Terror: The Elusive Nexus Between Public Access and Terrorist Attack

James T. O'Reilly

FOIA and Fighting Terror: The Elusive Nexus Between Public Access and Terrorist Attack

James T. O'Reilly[*]

I. INTRODUCTION

How much should our society change to fight terrorism and still maintain our traditions and rights? Information is power, and less information is flowing *out* of government as more information has been flowing *in*. Is this a serious trend or a misperception? In my corner of administrative law, amid the Freedom of Information Act (FOIA) and privacy legislation aficionados, there is a raging storm of contrary opinions that surfaces whenever our small band of disclosure advocates gets together, and we (being lawyers) cannot agree.

Picture the television commercials of cars with crash dummies hitting a wall. Our open society went suddenly from a trend of "everyone should get everything online that they ever could want to know" to the rapid deceleration—the slowdown of disclosure—that marks the foreseeable future response to Al Queda. The change is the brutal awakening to a new opponent seeking martyrdom, who was in Florida libraries and was downloading United States government website files. The enemy using our federal agencies' web disclosures is no longer a slow-moving, monolithic Kremlin seeking missile technology secrets with agents who can be pinpointed and sometimes offered asylum to switch to our side. The adversary is a mass movement of technically well-educated and very dedicated small cells of attackers using the internet, the library, and the news sources of the twenty-first century. Their goal is no longer to defend a land mass and a particular politburo. Rather, their goal is to use their martyrdom to force westerners into submission to a theocratic Taliban-like state, run on eighth century norms of societal subjugation. Suddenly, we are the infidels; we are the target of a six-foot five-inch Saudi millionaire with a masters in civil engineering and a devoted cadre of highly motivated and literate followers.

As the game has changed, the rules are changing. This paper represents a snapshot of that change as it relates to information exchange and disclosure. This paper proposes that we recognize that the retreat from pro-disclosure openness is underway; that the voters are tolerant, if not fully supportive, of federal secrecy; and that we should look to a new form of administrative surrogates for the resolution of disclosure disputes between government and citizens.

---

* Volunteer Professor of Law, University of Cincinnati, College of Law.

II. BACKGROUND OF STATUTORY DISCLOSURE SYSTEMS

The FOIA[1] disclosure system was created between 1961 and 1964, and was premised on a "retail" style, one request at a time, disclosure system. The "wholesale" aspect of disclosure had already been required in the 1946 Administrative Procedure Act,[2] which had required all rules to be published. What was new about the 1966 FOIA[3] was its novel permission to individuals to obtain agency records on request unless one of nine exemptions[4] applied. The FOIA ideal was that "any person" could have access without explaining why.[5] During the development of the Act, the primary movers were the American Society of Newspaper Editors.[6] They considered having language that would give extra access rights for reporters or the media, but settled on the less objectionable view that all requesters of whatever background should be the democratically ideal audience for government information.

The first of several myths, which I call the "FOIA Fictions," was that any average person would be using the disclosure statute. The next twenty years showed that average users were not journalists or common citizens. It may be speculated (in the absence of a centralized statistical database report) who the FOIA users have been. It is my observation that convicted criminals in federal prisons and their defense counsel have been the largest identifiable class of requesters. These user statistics seem to be followed closely by requests from agents of corporations which opposed regulators, or argued about federal contract denials, or who wanted to study the competitors' application for a government license or approval. The third largest requesters may have been the Washington based advocacy groups, whose selective use of federal documents to blast federal agencies has frankly scared some agency employees out of using written advocacy for controversial proposals or innovative policy proposals. Fourth on the list may have been trade press and specialized news service reporters seeking insider information for publication to their insider audiences. A distant fifth or sixth were general journalists, and far back in the pack were average citizens who, for individual reasons, wanted to have some knowledge of a certain government program.[7]

---

1. 5 U.S.C. § 552 (2004).

2. Pub. L. No. 79-404, 60 Stat. 237 (1946) (codified as amended in scattered sections of 5 U.S.C.).

3. Pub. L. No. 89-487, 80 Stat. 250 (1966), *amended by* Pub. L. No. 89-554, 80 Stat. 383 (1966).

4. 5 U.S.C. § 552(b) (2004).

5. *Id.* § 552(a)(2).

6. This history is explained at length in 1 James T. O'Reilly, Federal Information Disclosure ch. 2 (3d ed. Supp. 2004).

7. This approximation of gross volume is necessarily subjective and speculative in the absence of a central source of user identities, and it omits the

What could this "any person" do with the records? Anything! The FOIA did not care. Indeed, it aggressively declined to consider motives of the first requester,[8] because once the record is released to any person, it is deemed no longer subject to an exemption from required disclosure.[9] An alleged terrorist could, and indeed, has sued for FOIA access to federal investigations of his work.[10] This blindness to motives was a conscious policy response against the perceived evils of selectivity in disclosure. The press had been denied more than selective, "leaked" records access in the 1950s,[11] so the press endorsed very un-selective access in the FOIA in the early 1960s. At the time, that was an understandable policy choice for the advocates of an openness proposal. The policy of "disclose to one, disclose to all" has continued for decades since, as a fundamental assumption of FOIA with rare exceptions.[12]

III. TRANSFORMATIVE EFFECTS OF THE INTERNET

What effect did the Internet have? In those glorious days of peace and harmony around 1996, when the most recent FOIA amendments were being adopted,[13] the emphasis was on pushing out the maximum set of records at maximum speed and with minimal transaction costs and minimal delays.[14] The Internet magnified the consequence of disclosure, from one person getting one sheet of paper, to millions of potential users world-wide downloading data and diagrams. We were naïve, and we assumed all consequences of disclosure were good. Parents of teenage drivers can relate to this feeling: the younger driver never experienced the consequence of inattention and cannot calibrate the potential harm of bad driving

---

requests that routinely are processed by agencies, such as veterans asking for benefits or social security recipients filing for retirement; those are not truly requesting information, but the informational record retrieval is counted as a FOIA request although it is part of the benefit transaction.

8. U.S. Dep't of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749, 109 S. Ct. 1468 (1989); Cooper Cameron Corp. v. U.S. Dep't of Labor, 280 F.3d 539, 547–48 (5th Cir. 2002).

9. 5 U.S.C. § 552(b)(1–9) (2004).

10. Doherty v. U.S. Dept. of Justice, 775 F.2d 49 (2d Cir. 1985).

11. The American Society of Newspaper Editors (ASNE) complaints about abuses by the Eisenhower administration are addressed in O'Reilly, *supra* note 6, § 2:2.

12. On rare occasions, Congress has selected recipient classes and denied access to others, e.g., a supporting file underlying the decision to license a new pesticide is accessible by United States firms but not by non-United States firms or their agents. 7 U.S.C. § 136a(g) (2004) , added by Pub. L. 95-396, 92 Stat. 831 (1978).

13. Pub. L. No. 104-231, 110 Stat. 3050 (1996).

14. *Id.*, *adopting* 5 U.S.C. § 552(f)(2) (2004).

habits. For example, the Clean Air Act of 1990 required analysis of the potential consequences of release of extremely hazardous chemicals.[15] The EPA thought it would help more people by requiring these to be posted on the Internet.[16] Opponents of secrecy did not accept the assertions that someone reading this Internet posting might want to actually cause the release to happen—that someone might want to sabotage a plant and spread a cloud of poison just where the mandatory analysis documents said it would go.[17]

We will never know if disclosure of a particular federal agency file on the Internet will allow that file to be used for an attack against the refinery, bridge, or other entity that is described in the file. We cannot tell. By its open nature, the Internet cannot tell us who has downloaded what records. In the old days, one could make an FOIA request for the agency log of FOIA requests, so as to track competitors' inquiries. That method of requesting and tracking was quaint, obsolete, and archaic; for today, the concept of "Internet data mining" of Internet files for competitive intelligence is taught quite openly around the world.

We heard during that pre-Internet era the FOIA Fiction was that citizens would benignly volunteer to make the requests and use the law to hold government accountable for government managers' behaviors. Instead, government has been a rich source of competitively valuable intelligence about competitive companies' permits and applications, plant inspections, and formulations. "Money talks and information walks" was the reality. In retrospect, federal agency accountability through right-minded FOIA requests by interested citizen-critics was a pleasant, obsolescent ambition from forty years ago.

IV. COSTS AND BENEFITS

It would be intriguing to see an update of the economists' evaluations of FOIA that were performed two decades ago.[18] What have we purchased for the eighty-two million dollars that the Justice Department spent on FOIA last year,[19] or the hundreds of millions devoted to FOIA in all of the agencies? You paid for at least one side of the litigation in each of the cases brought under FOIA; when the

15. 42 U.S.C. § 7412(r) (1999).

16. 40 C.F.R. § 1400 (RMP program).

17. Critics of nondisclosure argued vigorously for release. *See* S. Rep. 106-70, at 11-12 (1999).

18. William Casey, et. al., Entrepreneurship, Productivity & The Freedom of Information Act (1982).

19. U.S. Dep't of Justice, Annual Report on the Freedom of Information Act 2003, *available at* http://www.usdoj.gov/oip/annual_report/2003/03contents.htm.

federal agency loses, the court may award attorneys fees for the winning side,[20] and it seems to do so in just under half the cases where disclosures are made.[21] So what did the taxpayers get for their money? Since I started compiling my FOIA treatise in 1976, I have endeavored to read and summarize every reported FOIA decision; there have been a little over 5,000 decisions.[22] These 350 cases each year remain an important subset of administrative law jurisprudence. But have we seen the classic secrecy behaviors of bureaucrats change? Not so much. Has FOIA been a "weapon of mass instruction?" Not much. Some advocacy groups have embraced the public benefits of dissemination of data and their Internet websites are archives of embarrassing disclosures. Websites like bushsecrecy.org and ombwatch.org bravely reflect that mood of positive benefit from FOIA accessible records.

The claim that paying for all this FOIA litigation is worthwhile, because it changes bureaucratic behavior, has been another FOIA Fiction. The majority of agencies seem to have gone on with business as usual, with FOIA as a pesky occasional intrusion. The claim that the creation of the FOIA's right to sue for access would equalize the field and induce behavioral change has proven, unfortunately, to be another of the FOIA Fictions. It was true in 1965, but as FOIA became institutionalized, the bureaucratic coping mechanisms to deal with it have shielded the activities of the bureaucracy from any real impacts on behavior.

In practice, the significant wealth transfer that occurs because of FOIA does not help domestic productivity or the United States balance of payments. The Washington search firm which has sold FOIA research services since 1975 now prominently marks its billing documents for payment "in United States dollars only." The net outflow of useful, technological data from the Chinese government's publicly accessible websites is hard to guess, since that government tightly controls all aspects of the Internet. The amount of useful data from the United States websites that has been downloaded in China is probably in the millions of pages. The economists who predicted such wealth transfers from the FOIA in a book in 1983 were correct,[23] and would be even more correct since the Internet has accelerated the competitive utilization of agency files.

---

20. 5 U.S.C. § 552(a)(4)(E).

21. *See, e.g.*, Union of Concerned Scientists v. U.S. Nuclear Regulatory Comm'n, 824 F.2d 1219 (D.C. Cir. 1987) and cases reported in O'Reilly, *supra* note 6, § 8:28.

22. *See* U.S. Dep't of Justice, Office of Information & Privacy, Freedom of Information Case List (2002), *at* http://www.usdoj.gov/04foia/preface.pdf.

23. Casey, *supra* note 18.

The public's right to know anything anytime was an attractive ideal in the past, but now it is seen as "*So* September 10th!" What is the mood now after September 11th, and what does disclosure policy tell us about getting back to normal? I will offer five points for consideration:

1. Congress has led the retreat from full disclosure.
2. Federal courts have retreated in their interpretations of the breadth of exemptions in the disclosure statutes.
3. New postings of data are far more sensitive to misuse than ever before.
4. Public health is an area in which less disclosure is likely to occur.
5. The diminished public disclosure will make it difficult for both the terrorist and the concerned citizen to monitor local health issues.

Let me explain.

V. CONGRESS LED THE RETREAT

Congress has led the retreat from openness, though individual members have awakened to the consequences of the issue and are slowly speaking against the new requirements[24] with a kind of "buyer's remorse" for a bad bargain. Specifically, the USA PATRIOT legislation[25] added a new pair of reasons for not disclosing agency records. The Act also impacted disclosure policies in several minor ways.

The biggest change arose when Congress created a tailored exemption to the FOIA for a class of private data or local government planning data that could reflect vulnerability to terrorist attacks. This is the "Critical Infrastructure Information" (CII) exception to disclosure, created by section 214 of the Homeland Security Act.[26]

The elements of protected CII information are stated in the statute and closely followed in the Department of Homeland Security rules, which were published in interim final rule form in January 2003.[27] The final rules were issued in February 2004.[28]

---

24. H.R. 3171, 108th Cong., 1st Sess. (2003) (20 cosponsors for repeal of PATRIOT Act).
25. Pub. L. No. 107-56, 115 Stat. 272 (2001).
26. 6 U.S.C. § 133(a)(1)(A).
27. 68 Fed. Reg. 4055 (Jan. 27, 2003) (to be codified at 48 C.F.R. pt. 31).
28. 6 C.F.R. § 29, *adopted as* Final Rules, 69 Fed. Reg. 8073 (Feb. 20, 2004).

These include, under their protection, information voluntarily submitted to a covered federal agency for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose.[29] In literal text that statute includes as "Critical Infrastructure Information" any information (1) not customarily in the public domain, (2) related to the security of critical infrastructure or protected systems, and (3) within an enumerated broad category of types of records.[30] Once these criteria are met, then (4) the data recipient must be the Department of Homeland Security, which is the only federal agency covered by this provision;[31] (5) the agency must be acquiring the data for "use by that agency" rather than for other purposes or for dissemination to others;[32] (6) the document must be marked with the words specified in the statute for such express claims of CII status;[33] and (7) the submission must be voluntary, which is defined as "in the absence of such agency's exercise of legal authority to compel access to or submission of such information."[34] The implementing regulations adhere closely to the statutory text.[35]

---

29. Pub. L. No. 107-296, § 214, 116 Stat. 2135, 2152-55 (2002).

30. The statute, 6 U.S.C. §§ 131(3)(A), (B) and (C), requires that the information must relate to one of the following:

> (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;
>
> (B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or
>
> (C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation."

Id.

31. *Id.* § 131(2).

32. *Id.* § 133(a)(1)(A). If the Department of Homeland Security is merely the conduit for the FBI, for example, the conditions are not satisfied.

33. *Id.* § 133(a)(2)(A) ("This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002.").

34. *Id.* § 131(7)(A).

35. 6 C.F.R. § 29.1 (2004).

VI. PREEMPTING STATE DISCLOSURES

The new statute protecting CII also makes a dramatic and preemptive change from past disclosure laws because it directly blocks state and local disclosure laws. Access to government records is a statutory, rather than a constitutional right,[36] and both federal and state governments had enacted disclosure laws with different sets of protections. The federal FOIA has been interpreted by its 1962-65 founders[37] and its 1965-2002 judicial interpreters as applying only to federal records.[38]

The disclosure laws of the state and federal governments proceeded in parallel but different channels. State courts sometimes accepted arguments against disclosure of a state agency's file that was premised on a record's federally exempted status. But more often, state courts required a state record to be covered by a state law exemption if it was to be withheld. And at the state and local level, disclosure of records by helpful clerical employees in small offices has been the very casual norm, with few of the checkpoints that one encounters in the processing of federal FOIA requests.

Section 214 of the Homeland Security Act,[39] which created CII as a protected category, expressly preempts state or local laws allowing or requiring disclosure of items that are within this broadly defined set of security data. Section 214 bars disclosure under state and local FOIA statutes in the event that CII information is shared with a state or local agency.[40] The industry proponents see preemption as a necessary adjunct to the federal statutory purpose. Many chemical safety and explosives control data filings are made to both federal and state environmental agencies at the same time.[41] A terrorist's access anywhere is a loss to the security objectives. The CII proponents would argue that attacks can only be avoided if the unitary approach to preventing disclosure is maintained.

The Department of Homeland Security (DHS) rules on CII delegate the interpretation of the criteria to the private sector person who has a direct economic incentive not to allow disclosure to

---

36. Houchins v. KQED, 438 U.S. 1, 15, 98 S. Ct. 2588, 2597(plurality opinion) (quoting Potter Stewart, *Or Of the Press*, 26 Hastings L.J. 631, 636 (1975)).

37. O'Reilly, *supra* note 6, § 2:3.

38. Smith v. Herriott, 967 F.2d 591 (9th Cir. 1992); Ferguson v. Alabama Criminal Justice Information Center, 962 F. Supp. 1446 (M.D. Ala. 1997).

39. 6 U.S.C. § 133(a)(1)(A) (2004).

40. *Id.* § 133(c). Records independently obtained by the state or local entity under its own authority are not barred from disclosure by CII.

41. *See, e.g.*, Congress preserving state powers to demand submission of identical or greater volumes of chemical release risk data in 42 U.S.C. § 11041(a)(3) (2004).

competitors, local environmental advocates, plaintiffs' counsel, and potential attackers.[42] Critics will question whether CII statutory protection fully satisfies the requirements for coverage of Freedom of Information Act exemption (b)(3)(B). It will be asserted that the allocation of discretion about data coverage to the private data submitter, rather than to the agency manager, is a fatal flaw in the claim that the CII statute meets the FOIA (b)(3)(B) test. Opponents will argue that a vagueness of the coverage, combined with FOIA's explicitly pro-disclosure canons of interpretation, favors a finding that the CII clause is inadequate as an FOIA exemption under section (b)(3)(B) of FOIA.[43] One cannot expect busy federal judges to take the time to absorb these nuances. Many judges outside of Washington remain unfamiliar with FOIA, and some of these could side with the critics when reviewing the exemption claims *de novo* and without deference to the agency interpretation of the exemption.[44]

The desire for protection is not ended if FOIA (b)(3)(B) exemption does not apply. That status may not mean federal disclosure is mandated. The defending agency might be able to claim that the record was a commercial secret with potential competitive harm that was required to be submitted, and thus was not "voluntary." A voluntary submission under the CII statute[45] does not mean their submission was voluntary for purposes of FOIA exemptions dealing with commercial records confidentiality. Here, the fine points of statutory definitions will be crucial, for "voluntary" is a term of art in the field of federal information disclosure.[46]

The CII law may be vulnerable on state law grounds. Of course, if the state had power to get the same data and routinely compiled it, the CII legislation does not apply to such independently obtained records.[47] But if it is argued that CII cannot be disclosed under a state or city "open records" law, the state court challengers will attack the preemption authority of the Homeland Security Act provision.[48] They may prevail under current Supreme Court preemption jurisprudence if the express preemption assertions fail to

42. The Department's rules allow the submitter to make the determination of applicability of CII status to its plans or records, 68 Fed. Reg. 18,484 (Apr. 15, 2003).

43. 5 U.S.C. § 552(b)(3)(B) (2004).

44. *See* O'Reilly, *supra* note 6, § 8:12.

45. 6 U.S.C. § 133 (a)(7)(A) (2004).

46. Critical Mass Energy Project v. Nuclear Regulatory Comm'n, 975 F.2d 871 (D.C. Cir. 1992) (en banc) (voluntary status allows wider protections against disclosure). *See also*, O'Reilly, *supra* note 6, §14:70, for subsequent cases.

47. 6 U.S.C. § 133(c) (2004).

48. *Id.* § 133(a)(1)(E).

satisfy the Supremacy Clause[49] case law precedents.[50] State plaintiffs could assert their rights under existing state statutory access provisions, including the express "public right to know" access rights under systems in New Jersey[51] and other states.[52] Federal constitutional law demonstrates a presumption against preemption,[53] and Congress must be explicit in preempting a pre-existing state right such as a state statute that granted state disclosure rights to records required by a state. Since the statute excludes from CII records which were "independently" acquired by the state or local agency and thereby remain subject to state or local laws,[54] courts will only reach the constitutional preemption issue after determining the factual history of the acquisition of the particular records. The first state decision under this provision rejected a claim of CII status and declined to treat location of cell phone towers as being confidential.[55]

The Achilles heel of the new CII system is the local government clerical employee. The federal department may be slow in communicating to the tens of thousands of local offices that hold diagrams of dams, plans of refineries, lists of explosive storage sites, etc., that these offices are now barred from making their very routine disclosures under procedures that these employees have followed for decades. The private owner of the infrastructure information will have to engage in self-help, perhaps by requesting the local entities to change their disclosure practices. But this role is not mandated in the statute or in the regulations and would be a counter-intuitive action for a factory manager who needs to get along compatibly with the local zoning or buildings department.

VII. DELEGATING THE SHIELD POWER

Another weakness of the statute is its placement of the operational choice for CII into the hands of the private entity. A private firm can make a submission that triggers CII status or can undo the protective treatment with a selective written consent to

---

49. U.S. Const. art. VI, cl. 2.

50. See, generally, the Commerce Clause-Supremacy Clause conflicts in *U.S. v. Lopez*, 514 U.S. 549, 115 S. Ct. 1624 (1995).

51. N.J. Stat. Ann. §§ 34:5A-1–31(1984).

52. *See* James T. O'Reilly, *Technology and Trade Secrets*, 21 Seton Hall L. Rev. 64 (1990).

53. The best treatment of this issue is in Joseph Zimmerman, Federal Preemption: The Silent Revolution (1991).

54. 6 U.S.C. § 133(c) (2004).

55. Maine Public Utilities Comm'n, Order on Waiver, Dkt. 2001-284 (May 7, 2003).

dissemination.[56] The private entity gets to decide what it will treat as CII, and the department's rules state that it will accept the private choice.[57]

A commentary on CII history is necessary for background. The CII provision was one of several additions to the drafts of the Homeland Security Act as it was rapidly developed in 2001.[58] The FBI took as its drafting model the text of the compromise legislation adopted in 1999 for the shielding of certain maps of potentially dangerous chemical releases.[59] That legislation was sought by factory and refinery owners who feared that public dissemination of maps of the scenario of a "worst case" chemical leak,[60] under an EPA Clean Air Act[61] program, would broadcast the best ways for attackers to release such a cloud from a targeted factory. The Federal Energy Regulatory Commission (FERC), which controls both public power generating entities as well as the private energy industries, adopted a comparable CII program in 2003. FERC proposed to expand it to shield data that FERC rules required to be made available by companies directly to the public. But when compared with CII, the FERC's Order 630 had a more narrow coverage of infrastructure[62] and a more narrow withholding in its rules on posting of infrastructure information.[63]

VIII. IMPLEMENTING THE WILL OF CONGRESS

The Department of Homeland Security rules to implement this CII provision of the Act virtually track the text of the statute. DHS will rely on the discretion of the submitter as to whether the volunteered information meets the statutory definition.[64] There is no discretion to reject a claim, so there will be little or no base for

56. 6 U.S.C. § 133 (a)(1)(C) and (E)(ii) (2004).

57. 68 Fed. Reg. 18,484 (Apr. 15, 2003).

58. A fascinating unofficial narrative description of the statute's political backing is found in Steven Brill, After: How America Confronted the September 12 Era (2003).

59. Pub. L. No. 106-40, 113 Stat. 207 (1999). *See also* S. Rep. No. 106-70 (1999).

60. Risk Management Plans containing such maps had been required by EPA rules. 40 C.F.R. § 68.25 (2004). *See* Stephen Gidiere and Jason Forrester, *Balancing Homeland Security and Freedom of Information*, 16 Nat. Resources & Env't. 139, 144 (2002); James T. O'Reilly, *Access to Records versus Axis of Evil*, 12 Kansas J. Law & Pub. Policy 559 (2003).

61. 42 U.S.C. § 7412(r) (1999).

62. 18 C.F.R. § 388.113(c)(1) (2004).

63. 68 Fed. Reg. 9,857 (March 3, 2003) (making final the proposal from 67 Fed. Reg. 57,994 (Sept. 13, 2002)).

64. 68 Fed. Reg. 18,523 (Apr. 15, 2003), *amending* 6 C.F.R. § 29 (2004).

judicial deference if a challenger asserts that the decision to withhold CII in a particular case is arbitrary or an abuse of discretion. The issues of federal agency abdication of such a significant adjudicatory decision to an interested private party will be addressed in future litigation.

The process starts with the filing at the Department of Homeland Security of a piece of data that falls within the statutorily defined set of such information. If it is marked with the express claim of CII status, which is the trigger for confidentiality, that filing grants certain protections to the data or records against any public disclosure by any level of government.[65]

IX. CONGRESS ALSO SERVES "SUSHI"

Congress established an additional withholding category of "sensitive" but unclassified data.[66] One statutory change is called "sensitive homeland security information." This undefined set of records, nicknamed "SUSHI," is a new category not quite the same as classified military secrets, which have been exempt from FOIA disclosure since the beginning. The rules for this category are expected to be announced soon by the Department of Homeland Security, under powers delegated by the Homeland Security Act.

The information sharing provisions of the Homeland Security Act require the agencies to develop procedures by which they "identify and safeguard homeland security information that is sensitive but unclassified," and also share such information as appropriate for homeland security purposes.[67] An Executive Order may be issued to require agencies to safeguard sensitive homeland security information.[68] In a February 18, 2004 letter,[69] the Department of Homeland Security told an FOIA requester that no procedures have yet been finalized to implement this provision—section 892 of the Homeland Security Act. The Nuclear Regulatory commission is using this SUSHI approach to withhold submissions by licensed nuclear plants.[70]

---

65. 6 U.S.C. § 133(a) (2004).

66. *Id.* §§ 481–83, *adopted in* Homeland Security Act, Pub. L. No. 107-296, 116 Stat. 2135 (2001).

67. *Id.* §§ 892(a)(1)(A) and (B) (2004).

68. *See,* U.S. Dep't of Justice, Office of Information & Privacy, *FOIA Post* (2003), *at* http://www.usdoj.gov/oip/foiapost/mainpage.htm.

69. Letter from Elizabeth Withnell, Acting Dep't Disclosure Officer, Dep't of Homeland Security, to Steven Aftergood, Federation of American Scientists (Feb. 18, 2004).

70. Nuclear Regulatory Comm'n, Regulatory Guidance, 69 Fed. Reg. 40681, 40687 (July 6, 2004).

X. THE ADMINISTRATION ALSO SHRINKS DATA FLOWS

There are other indicators of the ways in which 9/11 changed moods. Automatic declassification of older records has been delayed several times. Executive Order 12,958 substantially altered the process for declassifying relatively old documents.[71] Records that were more than twenty-five years old, and have been determined to have permanent historical value, would have been automatically declassified whether or not the records have been reviewed. In 1999, however, President Clinton extended the time period for automatic declassification until October 17, 2001.[72] Before that deadline arrived, however, President George W. Bush further amended Executive Order 12,958 to extend the automatic declassification date until December 31, 2006.[73] So if the record was from 1979 and was a State Department cable related to terrorism, it remains classified today.

The 1996 FOIA amendments have been implemented with very little controversy up to this point.[74] These "E-FOIA Amendments" required the federal agencies to make "records created on or after November 1, 1996 . . . available, including by computer telecommunications."[75] Agencies already had a duty under the Paperwork Reduction Act's mandate to provide "timely and equitable access to the [data] underlying [public information] maintained in electronic format."[76]

As the White House directed, the Administration since 9/11 has been more careful about posting material. The Justice Department also has been instructing agencies to be more attentive to the terrorist utility of new postings.[77] Congress has led the retreat from the open FOIA with these statutory changes, but the follow-up work has been done by the Administration.

XI. THE COURTS ALSO RETREAT INTO DEFERENTIAL ACCEPTANCE

As Congress and the Administration have been moving, so federal courts have retreated in their interpretations of the statutes.

---

71. *See, e.g.*, Exec. Order. No. 12,958, 69 Fed. Reg. 19,825 §§ 3.3(e) and 3.6 (Apr. 17, 1995).

72. *See* Exec. Order No. 13,142, 64 Fed. Reg. 66,089 § 1 (Nov. 23, 1999).

73. *See* Exec. Order No. 13,292, 69 Fed. Reg. 66,089 § 3.3(a) (Mar. 25, 2003). *See also* Primorac v. CIA, 277 F. Supp. 2d 117 (D.D.C., 2003).

74. But see contract disputes after the new statute, addressed in *Information Handling Servs., Inc. v. Defense Automated Printing Servs.*, 338 F.3d 1024 (D.C. Cir. 2003).

75. 5 U.S.C. § 552(a)(2) (2004).

76. 44 U.S.C. § 3506(d)(1)(B) (2004).

77. U.S. Dep't of Justice, Office of Information & Privacy, *FOIA Post: Guidance on Homeland Security Information Issued* (2002), *at* http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm.

There is substantial deference already given to agencies; I estimate that agencies have won ninety percent of litigated FOIA cases on summary judgment motions based on agency affidavits about the documents being withheld.

We see indications after 9/11 that the FBI and CIA receive greater deference than before, when they decline to disclose records because of national security or homeland defense issues. The few courts that have mentioned this factor are too small in number to make a valid estimate of a trend, but I have not seen courts apply the critical assessment that they had previously applied to law enforcement affidavits in domestic investigatory files cases. A future law review study should retrospectively examine the D.C. District Court judges' receptivity to agency secrecy claims in summary judgment motions before and after 9/11.

XII. FARMING OUT THE SECRETS TO EVADE FOIA DISCLOSURE

The CII protections and exemptions from the Freedom of Information Act do not apply to information that stays outside the federal government since there is no FOIA obligation upon non-federal entities that hold information. If private sector data about a facility is submitted to agents that are doing government's work but are outside government, then the information remains beyond the reach of FOIA disclosure. Agencies involved with the nation's infrastructure are far more sensitive to the misuse of records than they have ever been before. The power generation infrastructure is very vulnerable to attack and its companies are right to be concerned. To avoid FOIA disclosure entirely, the government is now funding the private coalitions known as ISACs, the Information Sharing and Analysis Centers. The private coalition ISACs were created by Presidential Decision Directive (PDD) 63;[78] President Clinton accepted the suggestion of the Oklahoma City bombing study commission to create and use ISACs as a means to combat the increasing vulnerability of our nation's infrastructure.[79]

---

78. Presidential Decision Directive 63/NSC 63 (1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm [hereinafter PDD 63] (The Clinton Administration's Policy on Critical Infrastructure Protections).

79. President Clinton appointed a Commission on Critical Infrastructure Protection, Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 17, 1996), to analyze and assess the vulnerabilities of and threats to our nation's critical infrastructure. *Id.* These critical infrastructures included "telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government." *Id.* Further, the Order acknowledged that these threats came in the form of physical, electronic, radio-frequency, or computer-based threats. *Id.* Moreover, the President called for public and private sector efforts to develop strategies for protecting and assuring the continued operation of

Following 9/11, in Executive Order 13,231, President Bush extended and amplified PDD 63.[80]

PDD 63 envisioned a federally supported national structure for the coordinated partnership of public and private entities in an effort to protect critical infrastructure.[81] Before the Department of Homeland Security was created, ISACs reported to the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, who was tasked with implementing the Directive.[82] PDD 63 directed the Coordinator to encourage owners and operators of the nation's critical infrastructure to develop ISACs.[83] The information was to flow into the National Information Protection Center (NIPC), which was created to oversee these ISACs for both governmental agencies and private entities.[84] The Directorate for Information Analysis and Infrastructure Protection of the Department of Homeland Security has assumed the role of the former NIPC.[85]

Information sharing poses a risk for many private entities because of the disclosure mandates in federal and state disclosure laws, such as the FOIA. Private industry was concerned that maps and audits of its vulnerability to attack might be required to be released by the NIPC. This was the situation when nuclear plant vulnerability was studied by industry self-audits and access to those audits was hotly contested in the litigation that led to the *Critical Mass* decision in 1992;[86] a decision favoring confidentiality arrangements.

The establishment of various industry specific sector ISACs was a direct response to these desires for non-disclosure of data concerning vulnerabilities.[87] Each sector's ISAC allows private entities to share security information without governmental disclosure of the data. The fourteen ISACs are each directed by its membership; the common mission is to gather, analyze, and disseminate to its members a comprehensive view of vulnerabilities, threats, and incidents relevant to the ISAC sponsoring sector's physical and cyber infrastructure.[88] As a result, the information which comes to ISACs will be used to provide warnings, establish

---

the infrastructures. *Id.* at 37,348.

80. Exec. Order No. 13,231, 66 Fed. Reg. 53,063 (Oct. 18, 2001).

81. PDD 63, *supra* note 78, at Annex A.

82. *Id.*

83. *Id.*

84. *Id.*

85. The current organization and duties of this Directorate are described at http://www.dhs.gov/dhspublic. The Directorate uses SUSHI to shield its meetings from public view. *See* Notice of Meeting, 69 Fed. Reg. 54299 (Sept. 8, 2004).

86. Critical Mass Energy Project v. Nuclear Regulatory Comm'n, 975 F.2d 871 (D.C. Cir. 1992) (en banc).

87. PDD 63, *supra* note 78.

88. *Id.*

trends (in terms of type and severity), and share threats and solutions among the ISAC membership and the Department of Homeland Security. ISACs are also a mechanism for sharing recommended security practices and solutions among the members. PDD 63 recommended that eight sectors form ISACs, and it partnered each of them with a corresponding lead agency of the federal government.[89]

ISAC formation started slowly after PDD 63. The market competitors were hesitant to share internal information. However, since 9/11 and the creation of DHS, the original eight ISACs have been further redefined into fourteen sectors, and many have been realigned with new agencies.[90] Additional sectors, Public Health and Public Transportation, are also currently being developed.[91]

XIII. PUBLIC HEALTH INFORMATION IMPACTED BY THE POST–9/11 SHRINKAGE

Public health is an area in which less disclosure is likely to occur after 9/11 for several reasons. First, the weaknesses of hospital and health care organizations in dealing with bioterrorism will be surveyed by the ISAC for public health, and the results will be reported to states and the federal agencies such as the Department of Health and Human Services (HHS) and the Department of Homeland Security. But that vulnerability report will never be public since it will be held within the ISAC. Any "critical infrastructure" data will be exempt from FOIA requests if it were to be shared with federal

89. These eight sectors were defined and aligned as follows: 1) the Commerce Department, for information and communications; 2) the Treasury Department, for banking and finance; 3) the Environmental Protection Agency ("EPA"), for the water supply industry; 4) the Transportation Department, for aviation, highways, mass transit, pipeline, rail, and maritime; 5) the Justice Department, for emergency law enforcement services; 6) the Federal Emergency Management Agency, for emergency fire service and continuity of government services; 7) the Department of Health and Social Services, for public health services; and 8) the Energy Department, for electric power generation and distribution and oil and gas production and storage. *Id.*

90. The fourteen current federally recognized ISACs and their lead agency include: 1) Transportation, DHS; 2) Financial Services, the Treasury Department; 3) Information Technology, DHS; 4) Telecommunications, DHS; 5) Energy (oil and gas), Energy Department; 6) Electricity, Energy Department; 7) Chemical, EPA; 8) Water, EPA; 9) Food and Agriculture, Agriculture Department and Department of Health and Human Services; 10) State Government, DHS; 11) Emergency Fire Services, DHS; 12) Emergency Law Enforcement, DHS; 13) Real Estate, DHS; and 14) Research and Education Network, NASA.

91. The Public Health ISAC will be overseen by the Department of Health and Human Services. The Coast Guard fostered creation of the maritime sector ISAC with a detailed agenda featuring confidentiality of data. *See* Notice of Meeting, 69 Fed. Reg. 51097 (Aug. 17, 2004).

agencies, because it is covered by section 214 of the Homeland Security Act.[92] The actual reports might never even reach the department, if the ISAC for public health is created as has been expected. The ISAC would ordinarily hold the data, and it would never become a federal "record" for FOIA purposes.[93]

Major changes in disclosure of personal medical histories and individual health records have occurred in the past several years. The implementation of the Health Insurance Portability and Accountability Act (HIPAA)[94] by exhaustive federal regulations[95] has stopped the flow of health disclosures dramatically. The Privacy Act[96] and FOIA[97] already restricted the dissemination of health records as a voluntary choice of the federal agencies. Now, since so many hundreds of thousands of healthcare workers have been forced to sit through HIPAA training, "leaks" are far less likely to occur. Public access to anthrax preparedness information for Detroit, for example, would be far less likely to be made public; it might be held by the healthcare ISAC, or withheld as CII under its FOIA exemption as discussed above, or withheld as SUSHI, or if individual anthrax poisoning had occurred, might also be withheld under FOIA exemption (b)(6),[98] or by operation of the HIPAA prohibitions.[99] Overall, it is far less likely that healthcare data will be accessible to the general public.

XIV. IMPACTS ON HEALTH SYSTEMS ACCOUNTABILITY

A fifth issue is the diminished public disclosure concerning healthcare system risks. This erosion of external information will make it difficult for the journalist, the terrorist, or the individual person to monitor the performance of defensive strategies to reduce risks relating to anthrax, bioterrorism, or local health issues arguably related to homeland defense.

The receptivity of the public to a loss of disclosure is the most difficult aspect to quantify. If ninety-nine point nine percent of Americans have not made FOIA requests for records, is FOIA access capability still important to them? By analogy, an Associated Press story in March 2004 reported that nearly sixty percent of Americans

92. 5 U.S.C. § 552(b)(3) (2004).
93. As a private record, it is not accessible under FOIA as an "agency record" would be. *Id.* § 552(a)(3).
94. Pub. L. No. 104-191, 110 Stat. 1936 (1996).
95. 45 C.F.R. § 164.502 (2004).
96. 5 U.S.C. § 552(a) (2004).
97. *Id.* § 552(b)(6).
98. *Id.* This exemption shields medical privacy information.
99. 45 C.F.R. § 164.502 (2004).

surveyed said that "government should have access to personal information that companies collect about consumers if there is any chance it will help prevent terrorism."[100] The public is making a tradeoff of the lesser of two evils—more secrecy for more defense. As an elected official talking to my city's voters about their concerns, I perceive that people are less sensitive to privacy issues since 9/11, though it will take years of research and retrospective evaluation to quantify what appears to be a change in the public's perceptions and expectations. The lessened expectation of privacy during our post-9/11 years has the potential to affect the way we think about openness and government information in the future.

XV. STRIKING A BETTER BALANCE

We aspire to be an open society, even in the face of terrorism, and disputes will inevitably arise about what is being withheld and why. Currently disputes can be litigated, but federal court lawsuits are expensive, cumbersome, and take a long time to resolve on the crowded dockets of our district courts. Congress had once given FOIA cases special status to advance them ahead of other cases, but that provision was repealed in 1984.[101] We need to have a dispute resolution function that works in a timely manner. The remedy selected in 1963 Senate drafts of what became the FOIA was a federal district court civil action for injunctive relief,[102] with *de novo* judicial review[103]and in-camera inspection of the records by the judge.[104] This produced yet another FOIA Fiction: courts would scrutinize agency decisions in detail. The reality is that agencies win on the basis of affidavits that are rarely specific and rarely revealing, and judges decline to use their power of in-camera review of the actual documents except in rare cases. Courts have not been very receptive to FOIA cases outside the very busy District of Columbia; the average United States district judge rarely sees FOIA and defers to agency affidavits on eighty-five percent of the cases. So if you are negotiating for a release with an agency, you do not have an easy time.

Ideally, the FOIA dispute needs an alternative remedy with credibility, speed, clout, and results. This alternative dispute resolution project would mean administratively centralizing the power to override an agency's withholding decision. For example,

100. *Terror Developments Tuesday*, Cincinnati Enquirer, Mar. 31, 2004, at A5.
101. Former 5 U.S.C. § 552(a)(4)(D), *revoked by* Pub. L. 98-620, Title IV, § 402(2), 98 Stat. 3357 (1984).
102. 5 U.S.C. § 552(a)(4)(B) (2004).
103. *Id.*
104. *Id.*

if the Coast Guard declined to reveal the safety status of a barge terminal handling liquid propane, the denial could be sent to a disclosure monitor or ombudsman who would have the final say on whether the record should be released. Ideally this official would be in the National Archives and Records Administration rather than in the Justice Department, and would have sufficient staff and legal authority to do the job.

Canada has functioned quite well with this model since 1983.[105] Several states have experimented; the FOIA Commission in Connecticut[106] has been a model adjudicator of access disputes. New York has had a specialized Committee on Open Government for intra-governmental appellate review of withholding for many years.[107] My impression is that the investment has yielded great benefits at the state levels. The idea is not new at the federal level, having been studied by the Administrative Conference in the 1980s.[108] Such a neutral and dispassionate disclosure monitor outside the agency should be available at the federal level, in lieu of the current statutory appeal only within the agency. This alternative dispute resolution could perhaps begin with homeland security and defense records disputes.

The potential administrative appeals role of the disclosure monitor at the National Archives and Records Administration is a compromise between the inadequacies of the court review process and the genuine need for protection of the sensitive agency records that would harm the national interest if disclosed. The Justice Department had operated such a system in the 1970s, functioning like the Solicitor General does in deciding internally which agency withholding would be deemed justifiable, and refusing to defend in court agency FOIA withholding that was not well justified. That system was centered at the Justice Department's FOIA office; but, by contrast, a new monitor would be located at the National Archives and Records Administration, outside of the Justice Department to avoid the inherent conflicts that would otherwise exist in litigation preparation and implementation. Such a monitor role in an administrative appellate system would be far cheaper and faster than district court litigation. Its independence would also make it superior to the zig-zag changes that have occurred in Justice Department disclosure policies. Those policies have been altered in

105. Access to Information Act, R.S.C. 1985, ch. A-1, *available at* http://canada.justice.gc.ca/en/A-1/index.

106. Conn. Gen. Stat. § 1-206(b) (2004).

107. N.Y. Pub. Off. Law § 89(4)(a) (1993).

108. Mark H. Grunewald, *Freedom of Information Act Dispute Resolution*, 40 Admin. L. Rev. 1 (1988).

each of the past four changes of Administrations, calling for more secrecy under Republicans[109] and a presumption of disclosure under Democratic administrations.[110]

Before a non-court intermediary could resolve records secrecy disputes and override agency withholding, the FOIA administrative appeals step[111] would have to be amended, or the Administration would have to create this gatekeeper as designee of the head of the agency by an Executive Order that binds each executive branch agency.

Such a new system would require several key pieces of supporting data to justify its establishment:

1. The development of expertise of the adjudicator in FOIA and in the subject matters that come before the new office;
2. The development of trust and confidence in quality of the reviewing officials' ability and impartiality; and
3. The avoidance of backlogs (FOIA time delays already are tremendous,[112] disregarding the statutory 10/20 day norms,[113] so referrals to this adjudicator should not drag out for a longer time, compared to the current system).

XVI. CONCLUSION

Getting "back to normal" with an open disclosure attitude will take years, if it ever occurs. We can predict that Congress will stay the course and not revisit this balance, unless its leadership can be convinced about the need to change. The attitude of Congress toward reform legislation is driven by the desire for preservation of power and attraction of campaign money. Those forces will assure that information policy will see no real changes, until financial or political pressures produce a better atmosphere for change. So, the key decisional committees of the Congress are *NOT* hearing the opinions of the general public resonating with concern on the government

---

109. U.S. Dep't of Justice, Office of Information and Privacy, *FOIA Post: New Attorney General FOIA Memorandum Issued*, *available at* http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm.

110. *See, e.g.*, OMB Watch, *at* www.ombwatch.org.

111. 5 U.S.C. § 552(a)(6)(I) (2004) ("[H]ead of the agency" would be replaced by a description of the new monitor.).

112. Actual and average times for processing of FOIA requests are required to be reported in each federal agency's annual report on FOIA operations; for example, the median time of processing at the Food and Drug Administration was 44 days. *See* U.S. Food and Drug Administration, Annual Freedom of Information Act (FOIA) Report (2003), *available at* http://www.fda.gov/foi/annual2003.html.

113. 5 U.S.C. § 552(a)(6) (2004).

secrecy issues. There is no groundswell of opposition to the set of tradeoffs this article has discussed. Congress should not be expected to roll back the more secretive policies instituted by the Homeland Security Act.

In this climate we should not anticipate that statutory modifications will be made to define greater access rights, or even to institute a streamlined adjudicatory system to resolve access disputes more rapidly. Successful requests for FOIA access will remain difficult and perhaps unattainably complex for the average citizen. The vast majority of voters are not FOIA users, and they would be likely to passively accept the narrowing of FOIA access if it were said to be done in order to enhance assurance that the recipients of the federal file data could not use it to plan attacks against the United States. So, will America get "back to normal" for information policy? Probably not for the next decade; we should not waste the remainder of this decade waiting for those golden years of openness to reappear.